

Mark C. Mao, CA Bar No. 236165  
 Beko Reblitz-Richardson, CA Bar No. 238027  
**BOIES SCHILLER FLEXNER LLP**  
 44 Montgomery St., 41st Floor  
 San Francisco, CA 94104  
 Tel.: (415) 293-6800  
 mmao@bsfllp.com  
 brichardson@bsfllp.com

Jesse Panuccio (admitted *pro hac vice*)  
**BOIES SCHILLER FLEXNER LLP**  
 1401 New York Ave, NW  
 Washington, DC 20005  
 Tel.: (202) 237-2727  
 Fax: (202) 237-6131  
 jpanuccio@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891  
**SUSMAN GODFREY L.L.P.**  
 1900 Avenue of the Stars, Suite 1400  
 Los Angeles, CA 90067  
 Tel: (310) 789-3100  
 Fax: (310) 789-3150  
 abonnn@susmangodfrey.com

*Attorneys for Plaintiffs*

**UNITED STATES DISTRICT COURT  
 NORTHERN DISTRICT OF CALIFORNIA**

ANIBAL RODRIGUEZ, JULIEANNA  
 MUNIZ, ELIZA CAMBAY, SAL  
 CATALDO, EMIR GOENAGA, JULIAN  
 SANTIAGO, HAROLD NYANJOM,  
 KELLIE NYANJOM, and SUSAN LYNN  
 HARVEY, individually and on behalf of all  
 others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

William Christopher Carmody  
 (admitted *pro hac vice*)  
 Shawn J. Rabin (admitted *pro hac vice*)  
 Steven M. Shepard (admitted *pro hac vice*)  
**SUSMAN GODFREY L.L.P.**  
 1301 Avenue of the Americas,  
 32<sup>nd</sup> Floor  
 New York, NY 10019  
 Tel.: (212) 336-8330  
 bcarmody@susmangodfrey.com  
 srabin@susmangodfrey.com  
 sshepard@susmangodfrey.com

John A. Yanchunis (admitted *pro hac vice*)  
 Ryan J. McGee (admitted *pro hac vice*)  
 Michael F. Ram (admitted *pro hac vice*)  
 Ra O. Amen (admitted *pro hac vice*)  
**MORGAN & MORGAN**  
 201 N. Franklin Street, 7th Floor  
 Tampa, FL 33602  
 Tel.: (813) 223-5505  
 jyanchunis@forthepeople.com  
 rmcgee@forthepeople.com  
 mram@forthepeople.com  
 ramen@forthepeople.com

Case No.: 3:20-cv-04688

**PLAINTIFFS' OPPOSITION TO  
 GOOGLE'S MOTION TO DISMISS THE  
 FIRST AMENDED COMPLAINT**

The Honorable Richard Seeborg  
 Courtroom 3 – 17th Floor  
 Date: March 4, 2021  
 Time: 1:30 p.m.

## TABLE OF CONTENTS

MEMORANDUM OF POINTS AND AUTHORITIES.....	1
I.    INTRODUCTION.....	1
II.   FACTUAL BACKGROUND .....	3
A.    Google Intercepts Plaintiffs’ Communications with Apps Using Google Scripts Embedded in Firebase SDK .....	3
B.    Plaintiffs Did Not Consent to Google’s Interceptions During Periods When Plaintiffs Switched Off Web & App Activity .....	3
C.    The App Developers Also Did Not Consent .....	4
D.    Google Associates the Intercepted Data with Preexisting User Profiles and Sells Them to Advertisers for Billions of Dollars.....	4
ARGUMENT .....	5
I.    Plaintiffs Have Stated a Claim Under the Wiretap Act.....	5
A.    Google’s Consent Defense Is Meritless .....	5
1.    Google’s Consent Defense Is Premised on a Fallacy about Firebase SDK.....	5
2.    App Developers Did Not Consent.....	6
3.    Plaintiffs Did Not Consent .....	9
i)    The Apps’ Disclosures Did Not Inform Plaintiffs of Google’s Interception of Communications While Web & App Activity Was Switched Off .....	9
ii)   Google’s Disclosures Stated that Google Would Not Save Data While Web & App Activity Was Switched Off.....	10
iii)  Google Introduces a Product Not Referenced in the FAC .....	13
B.    Consent Is Irrelevant Because Google Intercepted the Communications with the Intent to Commit an Unlawful Act.....	13
1.    The Comprehensive Computer Data Access and Fraud Act (CDAFA) .....	14
2.    Intrusion Upon Plaintiffs’ Seclusion and the Constitutional Right to Privacy .....	14
3.    The FTC Consent Order .....	14
4.    The California Consumer Privacy Act (CCPA) .....	15

1	II.	Plaintiffs Have Stated Claims Under CIPA.....	15
2	III.	Plaintiffs Have Stated a Claim Under the CDAFA .....	17
3	IV.	Plaintiffs Have Stated Constitutional and Common Law Privacy Claims	
4		.....	18
5	A.	Plaintiffs Had a Reasonable Expectation of Privacy .....	19
6	B.	Google’s Conduct Is “Highly Offensive” .....	20
7	V.	Plaintiffs Have Stated an Unfair Competition Law (UCL) Claim .....	22
8	A.	Plaintiffs Have UCL Standing .....	22
9	B.	Plaintiffs Have Stated a UCL Claim Under the “Unlawful”	
10		Prong.....	24
11	C.	Plaintiffs Have Stated a UCL Claim Under the “Unfair” Prong .....	25
12	VI.	CONCLUSION .....	25

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**TABLE OF AUTHORITIES****Page(s)****Cases**

<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009) .....	5
<i>Bautista v. Valero Mktg. &amp; Supply Co.</i> , No. 15-CV-05557-RS, 2018 WL 7142094 (N.D. Cal. Dec. 4, 2018) (Seeborg, J.) .....	24
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	5
<i>Blaustein v. Burton</i> , 9 Cal. App. 3d 161 (Cal. Ct. App. 1970) .....	22
<i>Brodsky v. Apple Inc.</i> , 445 F. Supp. 3d 110 (N.D. Cal. 2020) .....	9, 17
<i>Campbell v. Facebook Inc.</i> , 77 F. Supp. 3d 836 (N.D. Cal. 2014) .....	7, 8, 9
<i>Cappello v. Walmart Inc.</i> , 394 F. Supp. 3d 1015 (N.D. Cal. 2019) (Seeborg, J.) .....	3, 22, 24, 25
<i>Davis v. Facebook, Inc.</i> , 956 F.3d 589 (9th Cir. 2020) .....	<i>passim</i>
<i>Facebook, Inc. v. ConnectU LLC</i> , 489 F. Supp. 2d 1087 (N.D. Cal. 2007) (Seeborg, M.J.) .....	18
<i>Flanagan v. Flanagan</i> , 27 Cal. 4th 766 (2002) .....	16
<i>Hameed-Bolden v. Forever 21 Retail</i> , 2018 WL 6802818 (C.D. Cal. Oct. 1, 2018) .....	15
<i>Henry Schein, Inc. v. Cook</i> , 2017 WL 783617 (N.D. Cal. Mar. 1, 2017) .....	18
<i>In re Anthem Data Breach Litigation</i> , No. 15-MD-02617-LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016) .....	23
<i>In re Carrier IQ</i> , 78 F. Supp. 3d 1051 (N.D. Cal. 2015) .....	18
<i>In re Facebook, Inc., Consumer Privacy User Profile Litig.</i> , 402 F. Supp. 3d 767 (N.D. Cal. 2019) .....	12, 23
<i>In re Google Assistant Privacy Litigation</i> , 457 F. Supp. 3d 797 (N.D. Cal. 2020) .....	17

1	<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.</i> ,	
	806 F.3d 125 (3rd Cir. 2015).....	19, 21
2	<i>In re Google Inc., (Gmail)</i>	
3	No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) .....	8, 9, 12
4	<i>In re Google, Inc. Privacy Policy Litigation</i> ,	
	58 F. Supp. 3d 968 (N.D. Cal. 2014).....	22
5	<i>In re iPhone Application Litigation</i> ,	
6	2011 WL 4403963 (N.D. Cal. Sept. 20, 2011).....	23
7	<i>In re iPhone Application Litigation</i> ,	
	844 F. Supp. 2d 1040 (N.D. Cal. 2012).....	22
8	<i>In re Maxim Integrated Prod., Inc.</i> ,	
9	No. 12-244, 2013 WL 12141373 (W.D. Pa. Mar. 19, 2013).....	14
10	<i>In re Nickelodeon Cons. Priv. Litig.</i> ,	
	827 F.3d 262 (3d Cir. 2016) .....	19, 20
11	<i>In re Vizio, Inc., Consumer Privacy Litig.</i> ,	
12	238 F. Supp. 3d 1204 (C.D. Cal. 2017).....	21
13	<i>In re Yahoo Mail Litig.</i> ,	
	7 F. Supp. 3d 1016 (N.D. Cal. 2014).....	19
14	<i>Kight v. CashCall, Inc.</i> ,	
15	200 Cal. App. 4th 1377 (Cal. Ct. App. 2011).....	2, 16
16	<i>Kindred Studio Illustration &amp; Design, LLC v. Elec. Commc'n Tech.</i> ,	
17	LLC, No. CV 18-7661-GW(GJSX), 2018 WL 6985317 (C.D. Cal. Dec. 3,	
	2018).....	25
18	<i>Low v. LinkedIn Corp.</i> ,	
	900 F. Supp. 2d 1010 (N.D. Cal. 2012).....	20
19	<i>Maghen v. Quicken Loans Inc.</i> ,	
20	94 F. Supp. 3d 1141 (C.D. Cal. 2015).....	10
21	<i>Manzarek v. St. Paul Fire &amp; Marine Ins. Co.</i> ,	
	519 F.3d 1025 (9th Cir. 2008) .....	5
22	<i>Matera v. Google Inc.</i> ,	
23	No. 15-CV-04062-LHK, 2016 WL 5339806 (N.D. Cal. Sept. 23, 2016) .....	5, 6, 15
24	<i>Mirkarimi v. Nevada Prop. 1 LLC</i> ,	
	2013 WL 3761530 (S.D. Cal. July 15, 2013).....	16
25	<i>Moreno v. San Francisco Bay Area Rapid Transit District</i> ,	
26	No. 17-CV-02911-JSC, 2017 WL 6387764 (N.D. Cal. Dec. 14, 2017).....	22
27	<i>Opperman v. Path, Inc.</i> ,	
	205 F. Supp. 3d 1064 (N.D. Cal. 2016).....	19
28		

1	<i>Oracle USA, Inc. v. Rimini St., Inc.</i> ,	
2	879 F.3d 948 (9th Cir. 2018) .....	17
3	<i>Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress</i> ,	
4	214 F. Supp. 3d 808 (N.D. Cal. 2016) .....	14
5	<i>Revitch v. New Moosejaw, LLC</i> ,	
6	2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) .....	17
7	<i>Smith v. Facebook, Inc.</i> ,	
8	262 F. Supp. 3d 943 (N.D. Cal. 2017) .....	19
9	<i>Sprewell v. Golden State Warriors</i> ,	
10	266 F.3d 979 (9th Cir. 2001) .....	16
11	<i>Troyk v. Farmers Grp., Inc.</i> ,	
12	171 Cal. App. 4th 1305 (Cal. Ct. App. 2009) .....	23, 24
13	<i>United States v. Christensen</i> ,	
14	828 F.3d 763 (9th Cir. 2015) .....	2, 18
15	<i>Watkins v. L.M. Berry &amp; Co.</i> ,	
16	704 F.2d 577 (11th Cir. 1983) .....	8
17	<i>Williams v. Facebook, Inc.</i> ,	
18	384 F. Supp. 3d 1043 (N.D. Cal. 2018) (Seeborg, J.) .....	18, 22
19	<i>Yunker v. Pandora Media, Inc.</i> ,	
20	No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) .....	22
21	<b>Statutes</b>	
22	18 U.S.C. § 2511(2)(d) .....	2, 5, 13
23	Cal. Bus. & Prof. Code § 17204 .....	22
24	Cal. Bus. & Prof. Code § 22576 .....	24, 25
25	Cal. Civ. Code § 1798.100(b) .....	15
26	Cal. Civ. Code § 1798.120(a) .....	22
27	Cal. Civ. Code § 1798.125(a) .....	22
28	Cal. Civ. Code § 1798.140(o)(1) .....	15
	Cal. Civ. Code § 1798.155 .....	15
	Cal. Penal Code § 502(c)(2) .....	14, 17
	Cal. Penal Code § 631 .....	15
	Cal. Penal Code § 632 .....	2, 15, 17
	California Privacy Rights Act .....	22

## MEMORANDUM OF POINTS AND AUTHORITIES

### **I. INTRODUCTION**

This case is about Google’s surreptitious interception and collection of highly personal data from consumers’ use of over a million software applications (“apps”) on their mobile devices. Google did this without consent with its Firebase Software Development Kit (“Firebase SDK”), after Plaintiffs had turned off a Google-offered consumer control called Web & App Activity.

The allegations demonstrating Google’s impropriety are straightforward. Google assured users that they could “adjust [their] privacy settings to control” the information Google collects. First Amended Complaint (“FAC”) ¶¶ 5, 67, 106. Google then invited users to exercise that control using Google’s Web & App Activity on/off switch. Google said this Web & App Activity feature “must be on” for Google to “save” “[i]nfo[r]mation] about [users’] browsing and other activity on . . . apps . . . that use Google services.” FAC ¶ 70. Google defined its “services” to “include . . . [p]roducts that are integrated into third-party apps.” FAC ¶¶ 5, 66. Consistent with those uniform Google representations, users switched off the “Web & App Activity” feature to prevent Google from collecting their sensitive information when they used third-party apps that integrated Google products. FAC ¶¶ 7, 201.

Google now concedes that its privacy controls actually do nothing. Mot. to Dismiss (“MTD” or “Motion”) at 1-2; FAC ¶ 6. Google continues to intercept users’ communications with apps after users switch off Google’s Web & App Activity feature. Contrary to Google’s representations, without notice or consent, Google uses secret scripts embedded within its Firebase SDK to collect data from user communications with the apps and send that data to Google servers, notwithstanding whether a user switched off Web & App Activity. FAC ¶¶ 3, 49, 52, 55-58.

Google’s Motion relies on two primary contentions, neither of which provide any basis to dismiss any of Plaintiffs’ claims. First, Google conflates Plaintiffs’ allegations on Firebase SDK with a different Google product called Google Analytics. Plaintiffs pled that Google Firebase SDK – not Google Analytics – intercepts user communications and data notwithstanding representations made by Google, and notwithstanding consumers turning off settings offered by Google. FAC ¶¶ 3, 6, 40, 42, 49, 52, 57. Google knows the two products are different, but

1 regardless, Google’s attempts to mischaracterize the case are simply improper.

2 Google’s other primary contention is that the apps consented to Google’s interception of  
3 the users’ communications. That is also false. Setting aside that Google’s entire consent defense  
4 is based on arguments relating to Google Analytics, not Firebase SDK, Plaintiffs pled that Google  
5 specifically assured apps that Google would adhere to its own privacy policies, wherein Google  
6 promised that users could stop Google’s collection of app activity by switching off Web & App  
7 Activity. FAC ¶¶ 5, 66-76, 104-10. Google fails to show the contrary, and instead, actually  
8 proffers exhibits demonstrating that Google assured app developers that consumers would retain  
9 control. MTD Exs. 1-A at 5, 2-A at 1. In any event, consent is no defense to Plaintiffs’ Wiretap  
10 Act claim because Google acted for unlawful purposes. *See* 18 U.S.C. § 2511(2)(d). Google’s  
11 unlawful purposes included misappropriating consumer data for its own use and to the detriment  
12 of consumers, in violation of numerous laws. FAC ¶¶ 3, 6, 111-25, 142, 179, 191-204, 267, 288.

13 Plaintiffs also bring claims under the California Invasion of Privacy Act (“CIPA”).  
14 Google’s argument that the communications are not “confidential” under CIPA § 632 rests on a  
15 misunderstanding of California law and disregard for Plaintiffs’ allegations. There is no  
16 requirement that the intercepted communications contain “personally identifiable information,”  
17 *Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1389 (Cal. Ct. App. 2011), but even if that were  
18 the law, Plaintiffs’ allegations suffice, FAC ¶¶ 45, 117-20.

19 Google’s response to Plaintiffs’ Comprehensive Computer Data Access and Fraud Act  
20 (“CDAFA”) claim is similarly contrary to California law. The Ninth Circuit has rejected the  
21 “circumvention” requirement that Google attempts to read into the CDAFA, *United States v.*  
22 *Christensen*, 828 F.3d 763, 789 (9th Cir. 2015), but even if there were such a requirement,  
23 Plaintiffs’ allegations satisfy it, FAC ¶¶ 3, 6, 51-58.

24 Plaintiffs also allege constitutional and common law claims. Plaintiffs had a reasonable  
25 expectation of privacy, both because of the “sensitive” nature of the intercepted data, and because  
26 Google “represented to the plaintiffs that their information would not be collected, but then  
27 proceeded to collect it anyway.” *Davis v. Facebook, Inc.*, 956 F.3d 589, 602-04 (9th Cir. 2020).  
28 Google’s “surreptitious data collection” is also highly offensive conduct. *Id.* at 606.

Finally, the foregoing violations each trigger liability under California’s Unfair Competition Law (“UCL”), and Google’s breach of its own Privacy Policy provides an additional basis for UCL liability. *See Cappello v. Walmart Inc.*, 394 F. Supp. 3d 1015, 1023-24 (N.D. Cal. 2019) (Seeborg, J.). Plaintiffs’ allegations establish standing and both unlawful and unfair conduct by Google in violation of the UCL. FAC ¶ 313.

## **II. FACTUAL BACKGROUND**

### **A. Google Intercepts Plaintiffs’ Communications with Apps Using Google Scripts Embedded in Firebase SDK**

Google intercepts the communications at issue in this lawsuit by way of software scripts (bits of code) that Google embeds within its Firebase SDK, used by over 1.5 million apps. FAC ¶¶ 43, 49-58. These Google scripts intercept, copy, and ultimately transmit to Google data reflecting the users’ communications with the apps. FAC ¶¶ 50-58. For example, these Google scripts cause Google to intercept communications revealing the screens on the app that the viewer selects; the content the user requests the app to display; the web address (the URL) of the content the user is viewing; and much more. FAC ¶¶ 50-58. These Google scripts also scrape the user’s device for additional information (*e.g.*, device identifiers that uniquely identify the user’s device, geolocation information, and Google’s other persistent identifiers) and then have the device transmit that additional information to Google along with the app-interaction data. FAC ¶¶ 45, 117-20.<sup>1</sup>

### **B. Plaintiffs Did Not Consent to Google’s Interceptions During Periods When Plaintiffs Switched Off Web & App Activity**

People care deeply about retaining control over the data showing their interactions with apps, particularly because such data reveals intensely private information, such as health information, sexual interests, and political views. FAC ¶¶ 7-8, 154-55, 201. Google said in its Privacy Policy that users can stop Google’s interception of that data: “across [Google’s] services,

---

<sup>1</sup> As these paragraphs in the FAC show, Plaintiffs’ complaint is about Google’s secret scripts within its Firebase SDK, regardless of whether Google Analytics is installed. If Google disputes whether Firebase SDK is the code collecting user communications, that is a factual dispute that is improper for the purposes of a motion to dismiss.

1 [users] can adjust [their] privacy settings to control what [Google] collects and how [their]  
 2 information is used.” FAC ¶¶ 66-67. Google instructed users to visit Google’s “My Activity”  
 3 webpage, which “allows [users] to review and control data that’s created when [they] use Google  
 4 services,” including “[p]roducts that are integrated into third-party apps.” FAC ¶¶ 66-68.

5 Google’s “My Activity” webpage contains a feature called Web & App Activity, which  
 6 contains an on/off switch. FAC ¶¶ 62, 70. Google says that switch “must be on” in order to “let  
 7 Google save” “info about your browsing and other activity on . . . apps . . . that use Google  
 8 services.” FAC ¶¶ 70-72. Google defines its “services” to include “[p]roducts that are integrated  
 9 into third-party apps.” FAC ¶¶ 5, 66, 70. Users with Android devices can also turn off the Web  
 10 & App Activity switch using their devices’ “Settings” menu. FAC ¶ 62. Plaintiffs turned off the  
 11 Web & App Activity feature to prevent Google from intercepting and collecting data from their  
 12 communications with apps. FAC ¶¶ 75-76. Because Plaintiffs were not even aware that these  
 13 communications were being intercepted by Google, Plaintiffs did not and could not have consented  
 14 to the interceptions. FAC ¶¶ 75-76.

### 15 **C. The App Developers Also Did Not Consent**

16 Nor did the third-party businesses (“app developers”) that created and maintained these  
 17 apps consent to Google’s interceptions. FAC ¶¶ 104-10. Google never disclosed to the app  
 18 developers that Google continued to intercept communications even after users switched off Web  
 19 & App Activity. FAC ¶¶ 109-10. To the contrary, Google assured app developers that Google  
 20 would adhere to its own privacy policies and various privacy laws—which include the assurances  
 21 to users that they “can adjust [their] privacy settings to control what [Google] collects and how  
 22 [their] information is used,” using “My Activity” and the Web & App Activity feature “to review  
 23 and control data that’s created when [they] use Google services,”—i.e., “[p]roducts that are  
 24 integrated into third-party apps.” FAC ¶¶ 5, 66-68, 104-10.

### 25 **D. Google Associates the Intercepted Data with Preexisting User Profiles and** 26 **Sells Them to Advertisers for Billions of Dollars**

27 Google’s surreptitious interception has allowed Google to generate billions of dollars in  
 28 additional advertising revenue each year. FAC ¶¶ 6, 120. Google creates and maintains “profiles”

on its users that contain all the data Google can collect about each user and the user’s devices. FAC ¶ 115. After intercepting and collecting data from users’ communications with apps, Google associates that data with Google’s preexisting profiles, thereby enriching those profiles with data Google was not supposed to have. FAC ¶¶ 114, 117, 120. Google charges advertisers and apps for Google services that target users based on this data. FAC ¶¶ 114-17, 120, 123-24.

### **ARGUMENT**

A motion to dismiss must be denied if the complaint “state[s] a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* The court must “accept factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

#### **I. Plaintiffs Have Stated a Claim Under the Wiretap Act**

Google admits that it intentionally intercepts Plaintiffs’ electronic communications. MTD at 3. Google thus relies entirely on the consent defense found in 18 U.S.C. § 2511(2)(d), for which “it is Google’s burden to prove consent.” *Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 5339806, at \*17 (N.D. Cal. Sept. 23, 2016). Google cannot meet its burden because (1) neither users nor app developers consented to Google’s interception of these communications, and (2) even if they had, consent is irrelevant when the interception, as here, occurs for unlawful purposes.

##### **A. Google’s Consent Defense Is Meritless**

###### **1. Google’s Consent Defense Is Premised on a Fallacy about Firebase SDK**

Google’s Motion is misleading from the start in that it conflates Google Analytics with Google’s Firebase SDK. MTD at 1, 3-5. As explained in the FAC, and recognized in the exhibits that Google appends to its Motion, the two products are not the same. FAC ¶¶ 42, 180; MTD Ex. 1-A at 2. Google Analytics is a reporting service Google provides to app developers; Google’s Firebase SDK is a set of tools used to build apps, which includes the Google scripts at issue in this lawsuit. FAC ¶¶ 3, 40, 42, 49-50. The scripts embedded in Firebase SDK allow Google to collect

1 user data directly from the user’s phone. The scripts cause the phone to ultimately transmit copies  
 2 of the user’s communications directly to Google. FAC ¶¶ 50-56, 118-20. This is the unlawful  
 3 “interception.” *Id.* Later, Google then shares some of the intercepted data with those app  
 4 developers who subscribe to Google Analytics. FAC ¶¶ 49-58; MTD Ex. 1-A at 2, 4. Google’s  
 5 own exhibits to the Motion indicate as much: Firebase SDK is the “software” that Google uses to  
 6 collect the information that Google later provides to app developers through Google’s Analytics  
 7 “service.” MTD Ex. 1-A at 1, 3-4. Accordingly, Firebase SDK, not Google Analytics, is the  
 8 Trojan horse by which Google collects user data across over a million apps, and this collection  
 9 occurs whether or not an app developer has enabled Google Analytics.

10 Having little to say about Firebase SDK, disclosures or otherwise, Google inappropriately  
 11 tries to redirect this case to its Google Analytics service so that it may rely on a few cherry-picked  
 12 disclosures about that service. MTD at 3-5, 9-10. In any event, whether one is talking about  
 13 Firebase SDK or Google Analytics, Google completely fails to establish consent to the  
 14 interceptions at issue. Instead, Google’s own documentation shows that Google promises user  
 15 control over the data collection process, but then disregards users’ efforts to exercise that control.<sup>2</sup>

## 16 2. App Developers Did Not Consent

17 As a threshold matter, Google mischaracterizes Plaintiffs’ allegations and the technical  
 18 process by which Google intercepts users’ communications with apps to obtain user data.  
 19 Plaintiffs’ claims are not based, as Google suggests, on app developers sending data to Google in  
 20 some separate transmission. MTD at 10. Instead, Plaintiffs detail how the embedded Google  
 21 scripts within Firebase SDK causes the user’s device to send a copy of the data directly to Google’s  
 22 servers. FAC ¶¶ 3, 49, 52, 55-58; *see also Davis*, 956 F.3d at 608 (describing similar process).

23 Regardless, app developers did not consent to Google’s interception, and could not have  
 24 consented, because Google never told them that Google continues to intercept communications  
 25 from users who switched off the Web & App Activity feature. FAC ¶¶ 104-10. To the contrary,  
 26 Google told app developers that it would comply with its privacy policy, including representations

27 <sup>2</sup> Google’s Motion also ignores that “consent is usually a question of fact, where a fact-finder needs  
 28 to interpret the express terms of any agreements to determine whether these agreements adequately  
 notify individuals regarding the interceptions.” *Matera*, 2016 WL 5339806, at \*17.

1 regarding Google’s Web & App Activity feature. FAC ¶¶ 104-08.

2 Google’s Motion primarily relies on two disclosures: the Google Analytics for Firebase  
3 Terms of Service, and the Google Analytics for Firebase Use Policy. MTD at 3-4, 9-10 (citing  
4 MTD Exs. 1-A, 2-A). Setting aside that these disclosures focus on Google Analytics and not  
5 Firebase SDK, these two disclosures actually undermine Google’s consent defense. The Google  
6 Analytics for Firebase Use Policy explains that “App Users can opt-out of the Google Analytics  
7 for Firebase features . . . including through applicable device settings.” MTD Ex. 2-A at 1.  
8 Google’s Web & App Activity feature is one such setting. FAC ¶¶ 60-63, 69, 71. Thus, this  
9 Google document reinforces Plaintiffs’ allegations, and app developers’ understanding that  
10 Google was *not* collecting this data from users who switched off this feature.

11 Similarly, the Google Analytics for Firebase Terms of Service, MTD Ex. 1-A at 5, directs  
12 apps to a Google webpage stating users can “control the information collected by Google on . . .  
13 sites and apps . . . that use Google’s services” through “My Activity [which] allows [users] to  
14 review and control data that’s created when you use Google services, including the information  
15 we collect from the sites and apps you have visited,” MTD Ex. N at 2-3.<sup>3</sup> Here again, this  
16 document indicates that users can switch off Google’s data collection using Web & App Activity,  
17 undermining any claim that apps consented to Google’s interceptions.

18 These two documents support Plaintiffs’ allegations, showing that app developers  
19 consented to Google’s interception of only *some* user communications, namely those that the user  
20 had consented to by switching on Web & App Activity. Nothing in these documents “constitute[s]  
21 consent to the specific practice alleged in this case,” i.e., intercepting communications from users  
22 who switched off Web & App Activity. *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 847-48

---

23  
24 <sup>3</sup> Google conflates Exhibit N with Google’s Privacy Policy. *See* MTD at 10. Exhibit N is a  
25 separate webpage that was not referenced in the FAC and therefore is not properly before the  
26 Court. Even if it were admissible at this stage, Exhibit N does not establish consent because it  
27 indicates that the “My Activity” feature could prevent Google from intercepting users’  
28 communications with sites and apps. Google’s reliance on Exhibit O is equally misplaced. *See*  
MTD at 10. Exhibit O says that app developers can “temporarily or permanently disable collection  
of Analytics data . . . to fulfill legal obligations.” MTD Ex. O at 1. That does not foreclose *users*  
from being able to do the same (such as by switching off Web & App Activity), and Google’s  
other disclosures inform app developers of that very point. FAC ¶¶ 104-10.

(N.D. Cal. 2014). “[C]onsent is not an all-or-nothing proposition.” *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at \*12 (N.D. Cal. Sept. 26, 2013) [hereinafter *Gmail*].

Google also lacks any implied consent. “Consent . . . is not to be cavalierly implied” because doing so would “thwart” the Wiretap Act’s “strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place.” *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir. 1983). This District has accordingly “cautioned that implied consent applies only in a narrow set of cases.” *Gmail*, 2013 WL 5423918, at \*12 (citing *Watkins*, 704 F.2d at 581). Implied consent, like express consent, “is not an all-or-nothing proposition.” *Gmail*, 2013 WL 5423918, at \*12; *see also Campbell*, 77. F. Supp. 3d at 847-48 (rejecting implied consent defense because the defendant did not establish “consent to the specific practice” being challenged). “The critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception.” *Gmail*, 2013 WL 5423918, at \*12. Here, because there is no basis to infer that the app developers were even aware of the challenged practice, implying consent would “thwart” the Wiretap Act’s “strong purpose to protect individual privacy.” *Watkins*, 704 F.2d at 581.

Because Google cannot establish consent as a matter of law, Google mischaracterizes Plaintiffs’ allegations. According to Google, Plaintiffs “alleg[e] that Google’s disclosures to apps make plain that Google-account level settings, such as WAA, do not affect Firebase’s data collection.” MTD at 10 (citing FAC ¶ 58). That is simply inaccurate. Paragraph 58 does not even mention any disclosures. And Google has not cited any disclosures that show that app developers knew that Google-privacy controls, such as Web & App Activity, do not actually stop Firebase SDK data collection. To the contrary, the exhibits Google appends to its Motion show that Google promised that it would not collect data from users who switched off Web & App Activity. *See* MTD Exs. 1-A, 2-A. Regardless, Google’s desperate attempts to introduce “facts” based on repeated misreadings of its own disclosures are inappropriate for a motion to dismiss.

1                   3.     Plaintiffs Did Not Consent

2                   i)     *The Apps' Disclosures Did Not Inform Plaintiffs of Google's*  
 3                         *Interception of Communications While Web & App Activity Was*  
 4                         *Switched Off*

5             Google's principal argument is that Plaintiffs consented because Google purportedly  
 6     required app developers to disclose their use of Google Analytics to users, and users were required  
 7     to agree to the apps' terms of use and privacy policies. MTD at 4-5, 11. For support, Google  
 8     submits disclosures from 9 of the 1.5 million apps that use Firebase SDK. MTD at 4, 11; FAC ¶¶  
 9     43, 205. Google's reliance on these disclosures is unavailing for at least three reasons.

10            First, none of the nine disclosures that Google attaches to its Motion inform users that by  
 11    engaging with these apps, the users will undo the steps they already took to prevent Google from  
 12    tracking them, such as by switching off Web & App Activity. Accordingly, nothing in these  
 13    disclosures establish Plaintiffs' "consent to the specific practice alleged in this case." *Campbell*,  
 14    77 F. Supp. 3d at 847-48; *see also Gmail*, 2013 WL 5423918, at \*12. Second, these disclosures  
 15    refer to Google Analytics, a separate service that Google sells to some app developers. None  
 16    inform Plaintiffs about the specific Google Firebase SDK scripts that transmit data to Google  
 17    directly through the user's device. FAC ¶¶ 40, 42, 49-58; MTD Ex. 1-A.

18            Third, Google is wrong when it asserts that "[t]hese nine apps are the only apps relevant to  
 19    Plaintiffs' claims." MTD at 3. Over 1.5 million apps use Firebase SDK. FAC ¶ 205. Numerous  
 20    other apps on Plaintiffs' devices likely use Firebase SDK scripts, which transmit Plaintiffs' app-  
 21    interaction data to Google. Plaintiffs identified more than 400 apps that they use (FAC ¶¶ 207,  
 22    209, 211, 213, 215, 217, 219, 221, 223) but Plaintiffs do not (yet) know which apps contain these  
 23    secret Google scripts because Google does not publicly disclose which apps use Firebase SDK  
 24    (FAC ¶ 205) and Google has so far refused to provide Plaintiffs with this information in discovery.

25            Google's reliance on *Brodsky* and *Maghen* is misplaced. *See* MTD at 11, 14. In *Brodsky*  
 26    *v. Apple Inc.*, the court rejected the plaintiffs' "bald assertions . . . that they did not consent" to the  
 27    challenged practice, where the plaintiffs "offer[ed] no information" about the disclosures that  
 28    purportedly misled them. 445 F. Supp. 3d 110, 123 (N.D. Cal. 2020). Here, Plaintiffs have offered

1 detailed information about Google’s disclosures which specifically state that Web & App Activity  
 2 can be used to stop tracking of user-app interactions. *Maghen v. Quicken Loans Inc.* is even further  
 3 afield; the plaintiff did not dispute that the defendant’s policies adequately disclosed the challenged  
 4 practice. 94 F. Supp. 3d 1141, 1145 (C.D. Cal. 2015).

5 *ii) Google’s Disclosures Stated that Google Would Not Save Data*  
 6 *While Web & App Activity Was Switched Off*

7 Throughout the Class Period, Google prominently published at least two uniform  
 8 disclosures regarding the effect of switching off the Web & App Activity feature. First, in its  
 9 Privacy Policy, Google promised that:

- 10 • “[A]cross ***our services***, you can adjust your privacy settings to ***control what we collect*** and  
 how your information is used.”
- 11 • “‘My Activity’ allows you to review and control data that’s created when you use ***Google***  
***services*** . . . .”
- 12 • “***Our services*** include . . . [p]roducts that are integrated into third-party apps and sites, like  
 ads . . . .”

13 FAC ¶¶ 5, 66-68; FAC Ex. A at 1, 9 (emphases added). Google’s “services” therefore include  
 14 Firebase SDK.

15 Second, on Google’s “My Activity” webpage, which is the webpage that houses the Web  
 16 & App Activity on/off switch, a “Learn more” hyperlink placed just under the Web & App Activity  
 17 switch directs users to a webpage titled “See & control your Web & App Activity.” FAC ¶¶ 70-  
 18 71. On that webpage, Google explains that users can prevent Google from saving information  
 19 about users’ activity on third-party apps:

- 20 • “What’s saved as Web & App Activity. . . Info about your browsing and other activity on  
 21 sites, ***apps***, and devices ***that use Google services***” is “saved as Web & App Activity.”
- 22 • “To let Google save this information: Web & App Activity must be on.”

23 FAC ¶ 70. Google thus states that “Web & App Activity must be on” for Google to “save . . .  
 24 information” “about your browsing and other activity on . . . apps . . . that use Google services.”  
 25 FAC ¶ 70. “Google services” includes “products that are integrated into third-party apps,” such  
 26 as Firebase SDK. FAC ¶¶ 66-68; FAC Ex. A at 1. Users who access “My Activity” through their  
 27 Android mobile phones receive the same disclosures. FAC ¶¶ 71-72. These users are also  
 28 informed that the “Activity controls” menu of their devices, i.e., where the Web & App Activity

1 switch is housed, allows users to “[c]hoose the activities and info you allow Google to save.” FAC  
 2 ¶¶ 62, 71. Based on these disclosures, Plaintiffs and Class members had the objectively reasonable  
 3 belief that Google would stop intercepting their communications and collecting app usage data  
 4 when “Web & App Activity” was switched off. FAC ¶ 75.<sup>4</sup>

5 Google’s response to these uniform disclosures is to reach outside the four corners of the  
 6 FAC to quote Exhibit N. Google contends that Ex. N “expressly carves out independent consent  
 7 given to third parties for the provision of data to Google as superseding.” MTD at 7 (citing MTD  
 8 Ex. N); *see also* MTD at 5 (citing Ex. N). Google incorrectly suggests that Exhibit N is Google’s  
 9 Privacy Policy. MTD at 7. It is not. *See supra* n.3. Even if Exhibit N were properly before the  
 10 Court on this Motion, this document proves nothing. Exhibit N does not state that apps can nullify  
 11 the effect of switching off Web & App Activity. Exhibit N states just the opposite: users can  
 12 “control the information that is shared by your device when you visit or interact with sites and  
 13 apps that use Google services,” including through the “My Activity” webpage. Ex. N at 2-3.

14 Google’s other response to the uniform disclosures referenced in the FAC is to argue that  
 15 users should have understood that the Web & App Activity switch only affected the information  
 16 that Google placed into a user’s “Google Account,” and that flipping the switch “off” had no effect  
 17 on Google’s voracious collection of data, or Google’s saving of that data in Google’s own closely  
 18 guarded user profiles (rather than in users’ “Google Accounts”). *See* MTD at 6-7. In other words,  
 19 Google’s argument is that users should know—without being told—that they have one “Google  
 20 Account” for purposes of Google’s phony privacy controls and then an undisclosed shadow  
 21 account for which privacy controls are meaningless. This disturbing argument is absurd, and it  
 22 provides no basis to dismiss any of Plaintiffs’ claims.

23 Google’s argument is directly contradicted by Google’s engineers, who have repeatedly  
 24 admitted that Google’s disclosures about the Web & App Activity feature are highly confusing  
 25 and insufficient. *See* FAC ¶¶ 36, 77 (quoting Google employees describing Google’s “overall  
 26

27 <sup>4</sup> Google claims that “nowhere do Plaintiffs allege that they saw the disclosures that form the basis  
 28 of their lawsuit” and that Plaintiffs only “argue generally that ‘users’ expected that Google would  
 stop collecting [the] data.” MTD at 12. Google is wrong. *See* FAC ¶ 75.

1 mess” with regard to “consent,” including remarks that Web & App Activity is “[d]efinitely  
2 confusing from a user point of view” and “difficult enough that people won’t figure it out”).

3 Moreover, Google’s argument is based on just one sentence of the “See & control your  
4 Web & App Activity” webpage, and this sentence describes not what happens when the Web &  
5 App Activity switch is “off” but rather what happens when the switch is “on.” Here is the sentence:

6 If Web & App Activity is turned on, your searches and activity from other Google  
7 services are saved in your Google Account, so you may get more personalized  
8 experiences, like faster searches and more helpful app and content  
recommendations.

9 MTD at 7 (citing FAC ¶ 81). This sentence cannot even begin to bear the weight Google places  
10 on it. Google’s Privacy Policy promised users that they could “control what we collect” (FAC ¶  
11 67), not just what is placed in a user’s Google Account. Google also promised that “[t]o let Google  
12 save” the data, “Web & App Activity must be on.” FAC ¶ 70. Google could have, but did not  
13 state that users were only choosing whether “to let Google place information in your Google  
14 Account.” The single sentence Google relies on cannot establish Google’s consent defense as a  
15 matter of law because this sentence does not come close to showing that Google’s interpretation  
16 of the Web & App Activity feature “is the only plausible interpretation.” *See In re Facebook, Inc.,*  
17 *Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019) (“[I]n the context  
18 of this motion to dismiss[,] the plaintiffs may be deemed to have consented to this arrangement  
19 only if [the defendant’s interpretation] is the only plausible interpretation.”).

20 *Gmail* is instructive. In that case, users alleged that Google illegally intercepted emails to  
21 and from Gmail users, and then used those emails to create user profiles and to send targeted  
22 advertising. 2013 WL 5423918, at \*13-14. This Court rejected Google’s consent defense,  
23 reasoning that “[n]othing in the [Privacy] Policies suggests that Google intercepts email  
24 communication in transit between users.” *Id.* Instead, the policies “obscure[d] Google’s intent to  
25 engage in such interceptions” by “explicitly stat[ing] that Google collects ‘user communications .  
26 . . to Google,’” which “could mislead users into believing that user communications to each other  
27 or to nonusers were not intercepted.” *Id.* at \*14. This case involves far more obfuscation than  
28 *Gmail*. Here, Google’s uniform disclosures “obscure[d] Google’s intent” and “misle[]d users” by

1 explaining that “‘My Activity’ allows you to review and control data that’s created when you use  
 2 Google services” and that “Web & App Activity must be on” for Google to “save” “info[rmation]  
 3 about your browsing and other activity on . . . apps . . . that use Google services.” FAC ¶¶ 66-68,  
 4 70; FAC Ex. A at 1, 9. These disclosures omitted any mention that this “control” was merely  
 5 limited to the information placed in users’ “Google Accounts,” and that no “control” was available  
 6 over the data Google collected for its own purposes.

7 *iii) Google Introduces a Product Not Referenced in the FAC*

8 Google also attempts to show Plaintiffs’ consent by means of the “Google Analytics  
 9 browser add-on” (MTD at 5, 7), a product nowhere mentioned in the FAC and which according to  
 10 its name focuses on browsers, not apps on mobile devices. Google suggests that the mere existence  
 11 of this “browser add-on” should have alerted users not to give any credence to Google’s statements  
 12 in its various privacy disclosures. This is nonsense. There is no admissible evidence before the  
 13 Court of what this “browser add-on” is or does, when it first came into existence, or how it could  
 14 possibly stop the collection of app and device data at issue. *See* Google’s Request for Judicial  
 15 Notice ¶ 10; MTD Ex. H. The existence of this “add-on” does not refute as a matter of law the  
 16 numerous representations Google made about the effect of switching off the Web & App Activity  
 17 feature. Furthermore, the browser-add-on only applies to Google Analytics, and Firebase SDK is  
 18 an entirely different product as aforementioned. *See supra* subsection I.A.1.

19 **B. Consent Is Irrelevant Because Google Intercepted the Communications with**  
 20 **the Intent to Commit an Unlawful Act**

21 Google’s Motion also fails because consent is not a defense where the “communication is  
 22 intercepted for the purpose of committing any criminal or tortious act in violation of the  
 23 Constitution or laws of the United States or of any State.” 18 U.S.C. § 2511(2)(d). Here, Google’s  
 24 “purpose” was to: (1) associate data from the intercepted communications with preexisting user  
 25 profiles to enrich those profiles; (2) to sell these profiles (or the use of these profiles) to advertisers;  
 26 and then (3) to send targeted advertisements to the users based on the collected data, in violation  
 27 of numerous laws. FAC ¶¶ 6, 111-25, 142, 179, 191-204, 267, 288. Google does not dispute that  
 28 a post-interception violation of the cited laws would trigger this exception. Nor does Google

1 dispute Plaintiffs’ factual allegations about Google’s post-interception conduct.

2 1. The Comprehensive Computer Data Access and Fraud Act (CDAFA)

3 The CDAFA makes it a “public offense” to “[k]nowingly access[] and *without permission*  
4 take[], cop[y], or *make[] use of* any data from a computer, computer system, or computer network.”  
5 Cal. Penal Code § 502(c)(2) (emphasis added); *see id.* § 502(d)(1) (violation of (c)(2) is a felony).  
6 Google’s copying (interception) of Plaintiffs’ communications, in and of itself, violated this  
7 statute. *See infra* Section III. In addition, Google’s *subsequent* “use” of the communications  
8 constituted additional, independent violations of the CDAFA, triggering the unlawful-purpose  
9 exception. *See* FAC ¶¶ 198-99; *In re Maxim Integrated Prod., Inc.*, No. 12-244, 2013 WL  
10 12141373, at \*15 (W.D. Pa. Mar. 19, 2013) (holding that a violation of the Computer Fraud and  
11 Abuse Act “is sufficient to satisfy the requirements of the crime-tort exception”).

12 2. Intrusion Upon Plaintiffs’ Seclusion and the Constitutional Right to Privacy

13 “[S]ubsequent disclosure of the contents of the intercepted conversations for the alleged  
14 purpose of *further* invading the [Plaintiffs’] privacy” is a tortious act that also satisfies the  
15 unlawful-purpose exception. *Planned Parenthood Fed’n of Am., Inc. v. Ctr. for Med. Progress*,  
16 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016). Plaintiffs’ app-interaction data, collected during those  
17 periods when Plaintiffs switched off the Web & App Activity feature, may reveal Plaintiffs’ sexual  
18 interests, dating preferences, and political or religious views, and much other “sensitive”  
19 information and “habits” they desire to keep private. FAC ¶¶ 7, 201; *see also Davis*, 956 F.3d at  
20 604. Google further intrudes upon Plaintiffs’ right to privacy when it sells this information to  
21 advertisers and uses the information to send targeted advertisements to Plaintiffs. FAC ¶¶ 200-04.

22 3. The FTC Consent Order

23 In 2010, the FTC charged Google with violating its privacy promises, and Section 5 of the  
24 Federal Trade Commission Act (“FTC Act”), in connection with the launch of a social network.  
25 FAC ¶ 29. The resulting order (the “FTC Consent Order”) requires Google to obtain “express  
26 affirmative consent” from each user “prior to any new or additional sharing” of that user’s  
27 information that is “a change from stated sharing practices in effect at the time [Google] collected  
28 such information.” FAC ¶ 29. When Google collected data from users who had switched off the

1 Web & App Activity feature, Google shared that data with third parties in a manner that violated  
 2 the FTC Order, thus triggering the unlawful-purpose exception. FAC ¶¶ 45, 195-97; *cf. Hameed-*  
 3 *Bolden v. Forever 21 Retail*, 2018 WL 6802818, at \*8 (C.D. Cal. Oct. 1, 2018) (claim for  
 4 “unlawful” conduct under the UCL can be predicated on an FTC Act violation); *see also infra*  
 5 n.11.

#### 6 4. The California Consumer Privacy Act (CCPA)

7 The CCPA requires Google to disclose, “at or before the point of collection,” the categories  
 8 of personal information it collects from consumers and the purposes for which that information is  
 9 collected. Cal. Civ. Code § 1798.100(b). The CCPA also forbids Google from “us[ing] personal  
 10 information collected for additional purposes without providing the user with notice consistent  
 11 with this section.” Cal. Civ. Code § 1798.100(b). “Personal information” includes browsing  
 12 communications. Cal. Civ. Code § 1798.140(o)(1). Here, Google intercepted the communications  
 13 with the intent to (and did) “use” the data “for additional purposes without providing the consumer  
 14 with notice.” FAC ¶¶ 192-94. This violation is a tortious act. *See* Cal. Civ. Code § 1798.155.

## 15 **II. Plaintiffs Have Stated Claims Under CIPA**

16 Google’s interception of Plaintiffs’ communications also violated sections 631 and 632 of  
 17 the California Invasion of Privacy Act (“CIPA”). The CIPA requires that *all* parties consent to an  
 18 interception. *Matera*, 2016 WL 5339806, at \*16; Cal. Penal Code §§ 631(a), 632(a). Google  
 19 cannot prevail on its consent defense (MTD at 13-14) because neither Plaintiffs nor the apps  
 20 consented. *See supra* Section I.A. Google also argues that “‘GA for Firebase’—like a  
 21 dictaphone—cannot face liability under Plaintiffs’ CIPA claims” because GA for Firebase is a  
 22 “tool” or “device” and CIPA liability only extends to a “person.” MTD at 14. This is nonsense.  
 23 Plaintiffs have sued Google, based on its data collection using Firebase SDK, not “GA for  
 24 Firebase,” and Google is a “person” under CIPA. *See* Cal. Penal Code § 632(b) (defining “person”  
 25 to include a limited liability company).

26 Google next contends that Plaintiffs’ communications do not qualify as “confidential.”  
 27 MTD at 14-16. This argument applies only to section 632. A communication qualifies as  
 28 “confidential . . . if a party to that conversation has an objectively reasonable expectation that the

1 conversation is not being overheard or recorded.” *Flanagan v. Flanagan*, 27 Cal. 4th 766, 776-77  
 2 (2002). This test does *not* require the plaintiff to show an “additional belief that the information  
 3 would not be divulged [by the defendant] at a later time to third parties.” *Mirkarimi v. Nevada*  
 4 *Prop. 1 LLC*, 2013 WL 3761530, at \*2 (S.D. Cal. July 15, 2013); *see also Kight*, 200 Cal. App.  
 5 4th at 1397. Here, Plaintiffs reasonably expected that their communications were not being  
 6 overheard, recorded, or otherwise being saved by Google (or anyone) when they took the  
 7 affirmative step of turning off Web & App Activity. FAC ¶¶ 75, 202, 246-47, 281. This  
 8 expectation was reasonable because Google’s disclosures promised that users could prevent  
 9 Google from “sav[ing]” their data by switching off Web & App Activity. FAC ¶¶ 65-76.

10 Unable to dispute Plaintiffs’ factual allegations, Google instead tries to rewrite the law.  
 11 Google suggests that Plaintiffs must allege that the communications contained “personally  
 12 identifiable information.” MTD at 15-16. Google does not even purport to cite a case to support  
 13 this proposition, nor could Google. *See Kight*, 200 Cal. App. 4th at 1389 (“[S]ection 632 prohibits  
 14 unconsented-to recording or monitoring regardless of the content of the conversation . . .”).<sup>5</sup> In  
 15 any event, Plaintiffs allege that the intercepted data reveals who the user is and where the user is  
 16 located. FAC ¶¶ 45, 117-20. Plaintiffs also allege that the data may reveal a user’s sexual interests,  
 17 political or religious views, and private plans for the future (such as the purchase of an engagement  
 18 ring), among other desires, plans, and activities that users intended to keep private by switching  
 19 off the Web & App Activity feature. FAC ¶¶ 7, 201.<sup>6</sup>

20 Finally, Google buries within a parenthetical an argument that “*certain* electronic  
 21 communications [are] not confidential.” MTD at 15 (emphasis added). This is a truism, but the  
 22 particular communications *in this case* are confidential. The two cases that Google cites (without  
 23

24 <sup>5</sup> Instead, Google cites cases for the obvious proposition that “conclusory” allegations cannot be  
 25 credited. *See* MTD at 15-16. None of them addressed CIPA claims (nor any remotely analogous  
 26 factual scenario). *E.g., Sprewell v. Golden State Warriors*, 266 F.3d 979, 984 (9th Cir. 2001)  
 (addressing an NBA player’s challenge to a suspension he received for choking his coach).

27 <sup>6</sup> Google’s reliance on a policy prohibiting apps from sharing personally identifiable information  
 28 with Google is misplaced. MTD at 16. That policy is immaterial because the embedded Firebase  
 SDK code causes the user’s device to send the data directly to Google. FAC ¶¶ 49, 52, 55-58,  
 118-120. Regardless, Plaintiffs have pled that Google can identify users. FAC ¶¶ 45, 117-20.

discussion) do not undermine Plaintiffs' claims. *In re Google Assistant Privacy Litigation* did not even involve electronic communications. That case addressed *oral* communications that were mistakenly recorded, and the court dismissed the CIPA section 632 claim because the complaint "contain[ed] insufficient detail regarding the particular circumstances under which Plaintiffs used their Google Assistant Enabled Devices." 457 F. Supp. 3d 797, 816, 828 (N.D. Cal. 2020). Nor does *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) suggest that electronic communications cannot be confidential. In *New Moosejaw*, the defendant-website was in the business of selling clothing to consumers. The communications at issue were requests from the browser to view details about various items of clothing. *Id.* at \*1. The court held that "these particular internet communications" were not "confidential," *id.* at \*3 (emphasis added), thus verifying that electronic communications can be confidential in other circumstances.

### III. Plaintiffs Have Stated a Claim Under the CDAFA

Google's conduct also violated the CDAFA, which creates civil liability for anyone who "[k]nowingly access[es] and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2). Plaintiffs allege that Google acted without permission, including by creating "hidden" software code that, "without any notice to users," "secretly cop[ies] and transmit[s] . . . to Google" data about users' app usage, "render[ing] ineffective any barriers users may wish to use to prevent access to their information, including by turning off the 'Web & App Activity' feature." FAC ¶¶ 49, 54-58.

Google's "consent" defense (MTD at 19) fails. *See supra* Section I.A. Google's reliance on *Brodsky v. Apple Inc.* is once again misplaced. The *Brodsky* court rejected the plaintiffs' "boilerplate" allegations that Apple acted without permission, which "merely parrot[ed]" the statutory language. 445 F. Supp. 3d at 119, 132. Here, Plaintiffs have explained with specificity how Google acted without permission. Reliance on *Oracle USA, Inc. v. Rimini St., Inc.* is likewise misplaced because that case involved an entirely different issue: whether the defendant violated the CDAFA by using a non-approved method to access data it was generally permitted to access. 879 F.3d 948, 962 (9th Cir. 2018), *rev'd in part on other grounds*, 139 S. Ct. 873 (2019).

Equally unavailing is Google's argument that Plaintiffs do not allege that Google accessed

1 their data by “circumventing technical or code-based barriers.” MTD at 19-20. Most importantly,  
 2 the CDAFA is not limited to conduct that “circumvents” such “barriers.” In 2015, the Ninth Circuit  
 3 clarified that the CDAFA “does not require *unauthorized* access.” *Christensen*, 828 F.3d at 789  
 4 (emphasis in original). The “term ‘access’ as defined in the [CDAFA] includes logging into a  
 5 database with a valid password and subsequently taking, copying, or using the information in the  
 6 database improperly.” *Id.* Citing *Christensen*, courts have held that the CDAFA creates liability  
 7 even when a defendant does not circumvent a technical or code-based barrier. *See, e.g., Henry*  
 8 *Schein, Inc. v. Cook*, 2017 WL 783617, at \*5 (N.D. Cal. Mar. 1, 2017). Contrary to Google’s  
 9 representation, *Williams v. Facebook, Inc.* did not hold to the contrary. MTD at 19 (citing 384 F.  
 10 Supp. 3d 1043, 1053 (N.D. Cal. 2018) (Seeborg, J.)). The Court concluded only that “Facebook’s  
 11 averred exploitation of [a] permission setting on older Android OS devices” was “enough to plead  
 12 Facebook circumvented technical barriers in violation of the CDAFA.” *Id.* Google’s reliance on  
 13 *Williams* mistakes the sufficient for the necessary. *See also Facebook, Inc. v. ConnectU LLC*, 489  
 14 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007) (Seeborg, M.J.) (denying motion to dismiss CDAFA  
 15 claim where defendant “did not engage in ‘hacking’ or other ‘unauthorized’ access” but instead  
 16 “knowingly accessed [the plaintiff’s] website to collect, copy, and use data found thereon in a  
 17 manner not authorized or permitted by [the plaintiff]”).

18 In any event, Plaintiffs have alleged that Google circumvented various barriers. Google  
 19 embedded “hidden” software code into the apps, which caused Plaintiffs’ devices to send Google  
 20 a copy of the user-app communication and additional data scraped from the user’s device,  
 21 rendering ineffective Plaintiffs’ efforts to prevent access to their information. FAC ¶¶ 3, 6, 49-58,  
 22 117-20. That is sufficient. *See In re Carrier IQ*, 78 F. Supp. 3d 1051, 1101 (N.D. Cal. 2015)  
 23 (plaintiffs adequately alleged that the defendants acted “without permission” based on allegations  
 24 that “hidden” software transmitted data without notice or any way to stop the functionality).

#### 25 **IV. Plaintiffs Have Stated Constitutional and Common Law Privacy Claims**

26 Plaintiffs have also stated claims for intrusion upon seclusion and invasion of privacy.  
 27 “Because of the similarity of the tests, courts consider the[se] claims together and ask whether: (1)  
 28 there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive.” *Davis*,

1 956 F.3d at 601. Plaintiffs have met both elements.<sup>7</sup>

2 **A. Plaintiffs Had a Reasonable Expectation of Privacy**

3 Plaintiffs have alleged a reasonable expectation of privacy, both because of the highly  
4 sensitive nature of the intercepted communications *and* because Google led them to believe that it  
5 would not intercept these communications. *Davis* is instructive, addressing strikingly similar  
6 allegations, namely, that Facebook intercepted users' browsing communications with websites  
7 even after the users followed Facebook's instructions for how to prevent Facebook from tracking  
8 them. 956 F.3d at 602. Like Google, Facebook received copies of the communications through  
9 bits of embedded code, which caused the users' browsers to generate copies of the communications  
10 and transmit them to Facebook "through a separate, but simultaneous, channel in a manner  
11 undetectable by the user." 956 F.3d at 596, 607-08; FAC ¶¶ 3, 6, 49-58. Like Google, Facebook  
12 then "compile[d] these browsing histories into personal profiles which are sold to advertisers to  
13 generate revenue." 956 F.3d at 596; FAC ¶¶ 6, 111-25, 142, 179, 199. And like Google, Facebook  
14 first "set an expectation" with its users that this data would not be collected under certain  
15 circumstances (when users logged off Facebook), "but then collected it anyway." 956 F.3d at 602;  
16 FAC ¶¶ 4-6, 65-76.

17 The Ninth Circuit held that the plaintiffs had a reasonable expectation of privacy in their  
18 browsing communications. "[T]he critical fact was that [Facebook] represented to the plaintiffs  
19 that their information would not be collected, but then proceeded to collect it anyway." *Id.* at 603;  
20 *see also In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 293-95 (3d Cir. 2016) (holding, under  
21 analogous New Jersey law, that users had a reasonable expectation of privacy when Viacom  
22 promised that it would not collect particular information but then did); *In re Google Inc. Cookie*  
23 *Placement Consumer Privacy Litig.*, 806 F.3d 125, 151 (3rd Cir. 2015) (holding, under California

24 <sup>7</sup> Google's consent defense also fails. *See supra* Section I.A; *see also Opperman v. Path, Inc.*, 205  
25 F. Supp. 3d 1064, 1074 (N.D. Cal. 2016) (denying summary judgment on intrusion upon seclusion  
26 claim because a reasonable jury could find that the defendant's privacy policy "do[es] not  
27 explicitly address—and thus do[es] not obtain knowing consent for—" the challenged practice).  
28 By contrast, Google relies on cases in which the defendant's privacy policies explicitly disclosed  
the challenged practice. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017)  
(the defendant's data policy "disclose[d] the precise conduct at issue in th[e] case"); *In re Yahoo*  
*Mail Litig.*, 7 F. Supp. 3d 1016, 1029 (N.D. Cal. 2014) (users consented to the challenged practice  
based on the "clarity of the language in [the website's] disclosure").

1 law, that plaintiffs had a reasonable expectation of privacy based on allegations that Google evaded  
 2 browser-based cookie blockers even as “it held itself out as respecting” them). In addition, the  
 3 *Davis* court also held that the plaintiffs had a reasonable expectation of privacy because “Facebook  
 4 allegedly compiled highly personalized profiles from sensitive browsing histories and habits.” 956  
 5 F.3d at 604. Here, Google has similarly “compiled highly personalized profiles from sensitive  
 6 browsing histories and habits” after first “set[ting] an expectation” that Plaintiffs’ data would not  
 7 be collected when they switched off “Web & App Activity.” FAC ¶¶ 4-7, 65-76, 201.

8 Aside from its consent defense, Google’s only argument on this element is that Plaintiffs  
 9 do not allege that Google intercepted “objectively confidential” or “personally identifiable  
 10 information.” MTD at 17. This argument fails for the same reasons discussed above in the CIPA  
 11 section, particularly because the intercepted data reveals the user’s identity. FAC ¶¶ 45, 117-20;  
 12 *see also supra* Section II. More fundamentally, the standard for establishing a reasonable  
 13 expectation of privacy does not require plaintiffs to plead that the data was “personally  
 14 identifiable.” “[T]he critical fact was that [Google] represented to the plaintiffs that their  
 15 information would not be collected, but then proceeded to collect it anyway.” *Davis*, 956 F.3d at  
 16 603. Google’s reliance on *Low v. LinkedIn Corp.* is misplaced, particularly because *Low* predates  
 17 *Davis*. 900 F. Supp. 2d 1010 (N.D. Cal. 2012). Furthermore, the *Low* court merely concluded that  
 18 the plaintiffs did not have a reasonable expectation of privacy in the “limited information” that  
 19 LinkedIn collected, namely, “a user’s browsing history among LinkedIn profiles.” *Id.* at 1025,  
 20 1030. This case, by contrast, concerns sensitive data showing users’ detailed interactions with  
 21 millions of apps. *See* FAC ¶¶ 7, 45, 50-58, 201, 205.

## 22 **B. Google’s Conduct Is “Highly Offensive”**

23 Google’s conduct is also “highly offensive,” particularly because its “surreptitious”  
 24 interceptions target users’ sensitive interactions with millions of apps and can reveal users’ dating  
 25 activity, political or religious views, and myriad highly sensitive information. *Davis*, 956 F.3d at  
 26 606; FAC ¶¶ 7, 201, 205; *see also In re Nickelodeon*, 827 F.3d at 295 (concluding that Viacom’s  
 27 conduct was highly offensive insofar as Viacom “collect[ed] information using duplicitous  
 28 tactics”). Google promised that users could stop Google’s data collection by switching off the

1 Web & App Activity feature, but then Google intercepted Plaintiffs’ communications and collected  
 2 that data, and then used that data to profile and target Plaintiffs for advertisements. FAC ¶¶ 4-7,  
 3 65-76, 111-25, 142, 179, 191-204, 267, 288; *see Davis*, 956 F.3d at 606 (holding that “allegations  
 4 of surreptitious data collection” suffice for highly offensive conduct). That Google employees  
 5 recognize that Google’s privacy disclosures (including with Web & App Activity) are a “mess”  
 6 also suggests that Google’s conduct is highly offensive. FAC ¶¶ 35-36; *Davis*, 956 F.3d at 606.

7 Google contends that “there was no ‘invasion’ by Google at all” because the “apps used  
 8 GA for Firebase as a tool to analyze their users’ information.” MTD at 18. This argument is  
 9 foreclosed by *Davis*, which held that the plaintiffs adequately alleged privacy claims based on  
 10 interceptions that were facilitated by Facebook code that the websites embedded into their sites.  
 11 *See* 956 F.3d at 596, 608. This argument also (once again) misrepresents the technical process by  
 12 which Google receives the data. Google’s embedded code ultimately causes the user’s device, not  
 13 the apps’ servers, to independently send the data to Google. FAC ¶¶ 118-120.<sup>8</sup>

14 Google next argues that the “information at issue in this case is routine commercial  
 15 behavior that does not give rise to a ‘highly offensive’ invasion of privacy.” MTD at 18. The  
 16 Third Circuit (applying California law) has already rejected this exact argument, characterizing  
 17 the (purportedly) “routine” nature of such data tracking as an irrelevant “smokescreen.” *In re*  
 18 *Google Inc. Cookie*, 806 F.3d at 150. “[U]sers are entitled to deny consent, and they are entitled  
 19 to rely on the public promises of the companies they deal with.” *Id.* at 151; *see also In re Vizio,*  
 20 *Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (“[R]outine data  
 21 collection practices may be highly offensive if a defendant disregards consumers’ privacy choices  
 22 while simultaneously holding itself out as respecting them.”). The cases that Google cites predate  
 23  
 24  
 25

26 <sup>8</sup> This is clear from the graphic in paragraph 119 of the FAC. The intercepted communications  
 27 travel from the users’ devices to Google, not from the apps’ servers to Google. This process  
 28 resembles the challenged conduct in *Davis*, in which the plaintiffs alleged that the intercepted  
 communications traveled from the users’ browsers to Facebook, not from the websites’ servers to  
 Facebook. *Davis*, 956 F.3d at 596, 607-08.

*Davis*, and are factually distinguishable.<sup>9</sup> Furthermore, this Court has since rejected *In re iPhone Application Litigation* and *In re Google, Inc. Privacy Policy Litigation* as “unpersuasive” due to “their lack of consideration for California’s privacy norms.” *Williams*, 384 F. Supp. 3d at 1054.

#### **V. Plaintiffs Have Stated an Unfair Competition Law (UCL) Claim**

##### **A. Plaintiffs Have UCL Standing**

“[A] private [UCL] plaintiff must be able to show economic injury caused by unfair competition,” meaning “lost money or property.” *Cappello v. Walmart Inc.*, 394 F. Supp. 3d 1015, 1019 (N.D. Cal. 2019) (Seeborg, J.) (citing Cal. Bus. & Prof. Code § 17204). Plaintiffs have lost money or property in at least two ways, each of which is sufficient to assert this UCL claim.

First, Plaintiffs have standing under the UCL because Plaintiffs have a property interest in their data, and Google’s conduct has deprived them of that property and diminished its value. FAC ¶ 313; *see Walmart*, 394 F. Supp. 3d at 1019 (explaining that plaintiffs can establish UCL standing by “hav[ing] a present or future property interest diminished” or by “be[ing] deprived of money or property”). The CCPA, which was enacted in 2018 and took effect on January 1, 2020, provides consumers with the right to direct businesses to refrain from selling their personal information to third parties and prohibits companies from discriminating against consumers who exercise that right. Cal. Civ. Code §§ 1798.120(a), 1798.125(a). Accordingly, personal data now encompasses the “the legal right to exclude others,” which is “[a]n essential element of individual property.” *Blaustein v. Burton*, 9 Cal. App. 3d 161, 177 (Cal. Ct. App. 1970).

Following the enactment of the CCPA, the Ninth Circuit in *Davis* held that the plaintiffs “adequately pleaded an entitlement to Facebook’s profits from users’ personal data.” 956 F.3d at 600. And most recently, voters passed the California Privacy Rights Act (“CPRA”) in November

---

<sup>9</sup> The intercepted data in *In re iPhone Application Litigation* was not the “content” of any communication; it was “information about the identities of parties to a communication.” 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012). *Moreno v. San Francisco Bay Area Rapid Transit District* turned on the fact that the plaintiff was “on notice that [the defendant] would be accessing the information.” No. 17-CV-02911-JSC, 2017 WL 6387764, at \*8 (N.D. Cal. Dec. 14, 2017). In *Yunker v. Pandora Media, Inc.* the plaintiff failed to even allege that the defendant intercepted the communications at issue. No. 11-CV-03113 JSW, 2013 WL 1282980, at \*7 (N.D. Cal. Mar. 26, 2013). Finally, *In re Google, Inc. Privacy Policy Litigation* involved an amendment to Google’s privacy policy, which is inapposite here. 58 F. Supp. 3d 968, 974-75 (N.D. Cal. 2014).

2020, with the stated purpose of “further protect[ing] consumers’ rights, including the constitutional right of privacy.” CPRA § 3. The CPRA strengthens the data protections provided by the CCPA, explaining that “[c]onsumers should know who is collecting their personal information . . . , how it is being used, and to whom it is disclosed,” and that “[c]onsumers should be able to control the use of their personal information.” CPRA § 3.A.1-2.

Google counters that “numerous courts have held that a plaintiff’s ‘personal information’ does not constitute money or property under the UCL.” MTD at 21-22 & n.4 (citing cases). None of these cases addressed scenarios in which a plaintiff took concrete steps to protect particularly sensitive data. Moreover, all but one predate the CCPA, *Davis*, and the CPRA. The only exception is *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, and that case still predates the CCPA’s January 1, 2020 effective date. 402 F. Supp. 3d 767, 776 (N.D. Cal. 2019). *In re Facebook* is also distinguishable because the court’s sole reason for dismissing the UCL claim was that “the plaintiffs’ theory of economic loss [was] purely hypothetical.” *Id.* at 804. Here, by contrast, Plaintiffs allege that they paid money to the apps with the expectation that Google would abide by its promise to stop tracking users who turned off Web & App Activity. FAC ¶ 313.

Second, Plaintiffs have UCL standing because Plaintiffs paid for certain apps with the expectation that Google would not be able to collect data revealing their interactions with these apps while the Web & App Activity feature was switched off. FAC ¶ 313. These apps, in turn, used the money paid to them by Plaintiffs in order to pay Google for various services. Google then did precisely what Google promised not to do, i.e., Google collected data from users who had switched off Web & App Activity. FAC ¶ 313. Google contends that only money directly paid to the defendant is relevant for UCL standing (MTD at 21), but California courts have repeatedly rejected that argument.<sup>10</sup> The sole case upon which Google relies, *In re iPhone Application*

---

<sup>10</sup> “The UCL requires only that the plaintiff must once have had an ownership interest in the money or property acquired by the defendant through unlawful means.” *Troyk v. Farmers Grp., Inc.*, 171 Cal. App. 4th 1305, 1338, 1340 (Cal. Ct. App. 2009). In *In re Anthem Data Breach Litigation*, the plaintiffs had UCL standing even though they “might not have paid Defendants directly, [because] they nonetheless paid premiums which were then used to pay Defendants,” which meant that the plaintiffs sought “the return of money or property [that Defendants] acquired through its unfair

1 *Litigation*, did not hold to the contrary. There, the plaintiffs did not have standing under the UCL  
 2 because they did not allege that the money they paid to the apps had been redirected to the  
 3 defendant (Apple). 2011 WL 4403963, at \*14 (N.D. Cal. Sept. 20, 2011). There was “no nexus  
 4 between the alleged harm and Apple’s conduct.” *Id.* at \*6. Here, however, like the defendants in  
 5 *In re Anthem, Bautista, and Troyk*, Google has used unlawful means to acquire money from a third  
 6 party (the app developer) who had first obtained that money from Plaintiffs. The unlawful means  
 7 in this case is Google’s violation of various laws and, relatedly, its breach of its own Privacy  
 8 Policy. FAC ¶¶ 5, 65-76; *see also supra* subsection I.A.3.ii; *infra* Section V.B. “[A]n alleged  
 9 breach of the contractual terms of a privacy policy is sufficient to establish standing under the  
 10 UCL.” *Walmart*, 394 F. Supp. 3d at 1020.

#### 11 **B. Plaintiffs Have Stated a UCL Claim Under the “Unlawful” Prong**

12 “By proscribing ‘any unlawful’ business act or practice, the UCL ‘borrows’ violations of  
 13 other laws and treats them as unlawful practices that the UCL makes independently actionable.”  
 14 *Walmart*, 394 F. Supp. 3d at 1023. Plaintiffs allege that Google violated the UCL’s unlawful prong  
 15 by violating the Wiretap Act, CIPA, the CDAFA, the California Constitution’s right to privacy,  
 16 and the right to seclusion. FAC ¶ 307. Google does not dispute that these laws qualify as predicate  
 17 offenses. MTD at 22. In addition, Google’s breach of its Privacy Policy (*see supra* subsection  
 18 I.A.3.ii.) violated Section 22576 of the California Business and Professions Code, “which prohibits  
 19 a commercial website operator from ‘knowingly and willfully’ or ‘negligently and materially’  
 20 failing to comply with the provisions of its posted privacy policy.” *Walmart*, 394 F. Supp. 3d at  
 21 1023 (quoting Cal. Bus. & Prof. Code § 22576); *see also* FAC ¶ 307. Google does not dispute that  
 22 a violation of Cal. Bus. & Prof. Code § 22576 satisfies the UCL’s unlawful prong. Nor could

23 \_\_\_\_\_  
 24 practices.” No. 15-MD-02617-LHK, 2016 WL 3029783, at \*32 (N.D. Cal. May 27, 2016); *see*  
 25 *also Bautista v. Valero Mktg. & Supply Co.*, No. 15-CV-05557-RS, 2018 WL 7142094, at \*5 (N.D.  
 26 Cal. Dec. 4, 2018) (Seeborg, J.) (denying defendant’s motion for summary judgment on a UCL  
 27 claim where the plaintiff alleged that “the defendant indirectly obtained money from the plaintiff”);  
 28 *Troyk*, 171 Cal. App. 4th at 1338, 1340 (holding that the plaintiffs were entitled to seek restitution  
 under the UCL for money paid to a third-party because “it can be inferred a substantial portion of  
 the service charges paid by the class members to [the third-party] were indirectly received by [the  
 defendant] through payments made by [the third-party] to [the defendant] for services rendered”).

Google. *See Walmart*, 394 F. Supp. 3d at 1023 (“Plaintiffs adequately pled a violation of Section 22576, which is sufficient to state a UCL claim under the unlawful prong.”).<sup>11</sup>

### C. Plaintiffs Have Stated a UCL Claim Under the “Unfair” Prong

The “unfair” prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law. *Walmart*, 394 F. Supp. 3d at 1023. Some courts apply a balancing test, which requires courts to “weigh the utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” *Id.* Other courts apply a “tethering” test, under which the “unfairness must be tethered to some legislatively declared policy or proof of some actual or threatened impact on competition.” *Id.* Contrary to Google’s argument (MTD at 24), Plaintiffs allege facts establishing “unfair” Google conduct under either test. Google acted immorally and exclusively for its own benefit (obtaining billions of dollars in advertising revenue) while substantially intruding upon Plaintiffs’ right to privacy, including by surreptitiously collecting sensitive information that Plaintiffs intended to keep private. FAC ¶¶ 4-7, 201, 308-09. Specifically, Google’s violation of its Privacy Policy qualifies as “unfair.” *See Walmart*, 394 F. Supp. 3d at 1024. Plaintiffs’ UCL claim therefore “aligns with California’s policy of protecting customer data generally and holding companies accountable to their own privacy policies.” *Id.*

## VI. CONCLUSION

For the foregoing reasons, this Court should deny Google’s Motion to Dismiss in its entirety. If this Court disagrees, any dismissal should be without prejudice.

Dated: January 14, 2021

By: /s/ Amanda Bonn  
Amanda Bonn (CA Bar No. 270891)  
abonn@susmangodfrey.com  
SUSMAN GODFREY L.L.P.  
1900 Avenue of the Stars, Suite 1400  
Los Angeles, CA 90067

<sup>11</sup> Google contends that any violations of the FTC Act, FTC Consent Order, and the CCPA do not qualify as predicate offenses. MTD at 23. Google is wrong. *See Kindred Studio Illustration & Design, LLC v. Elec. Commc’n Tech., LLC*, No. CV 18-7661-GW(GJSX), 2018 WL 6985317, at \*7 (C.D. Cal. Dec. 3, 2018) (“Plaintiff may allege a UCL claim hinged on FTC Act Section 5, despite the fact [it] does not on its own provide a private right of action.”). In any event, this dispute is irrelevant because Google concedes that the other laws qualify as predicate offenses.

Telephone: (310) 789-3100

Mark C. Mao (CA Bar No. 236165)  
mmao@bsfllp.com

Beko Rebitz-Richardson (CA Bar No. 238027)  
brichardson@bsfllp.com

BOIES SCHILLER FLEXNER LLP  
44 Montgomery Street, 41<sup>st</sup> Floor  
San Francisco, CA 94104  
Telephone: (415) 293 6858  
Facsimile (415) 999 9695

Jesse Panuccio (admitted *pro hac vice*)  
jpanuccio@bsfllp.com

BOIES SCHILLER FLEXNER LLP  
1401 New York Ave, NW  
Washington, DC 20005  
Tel.: (202) 237-2727  
Fax: (202) 237-6131

James Lee (admitted *pro hac vice*)  
jlee@bsfllp.com

BOIES SCHILLER FLEXNER LLP  
100 SE 2<sup>nd</sup> Street, Suite 2800  
Miami, FL 33131  
Telephone: (305) 539-8400  
Facsimile: (305) 539-1307

William Christopher Carmody (*pro hac vice*)  
bcarmody@susmangodfrey.com

Shawn J. Rabin (*pro hac vice*)  
srabin@susmangodfrey.com

Steven Shepard (*pro hac vice*)  
sshepard@susmangodfrey.com

SUSMAN GODFREY L.L.P.  
1301 Avenue of the Americas, 32<sup>nd</sup> Floor  
New York, NY 10019  
Telephone: (212) 336-8330

John A. Yanchunis (*pro hac vice*)  
jyanchunis@forthepeople.com

Ryan J. McGee (*pro hac vice*)  
rmcgee@forthepeople.com

Michael F. Ram (*pro hac vice*)  
mram@forthepeople.com

Ra O. Amen (*pro hac vice*)  
ramen@forthepeople.com

MORGAN & MORGAN, P.A.  
201 N Franklin Street, 7th Floor

Tampa, FL 33602  
Telephone: (813) 223-5505  
Facsimile: (813) 222-4736

*Attorneys for Plaintiffs*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28